

SysAdmin's Notebook

Resetting a lost admin password

Periodically a situation arises where the FortiGate needs to be accessed or the admin account's password needs to be changed but no one with the existing password is available. If you have physical access to the device and a few other tools the password can be reset.

Warning:

This procedure will require the reboot of the FortiGate unit.

You will need:

- Console cable
- Terminal software such as Putty.exe (Windows) or Terminal (MacOS)
- Serial number of the FortiGate device

Step 1. Connect the computer to the firewall via the Console port on the back of the unit.

In most units this is done either by a Serial cable or a RJ-45 to Serial cable. There are some units that use a USB cable and FortiExplorer to connect to the console port.

Virtual instances will not have any physical port to connect to so you will have to use the supplied VM Hosts' console connection utility.

Step 2. Start your terminal software.

Step 3. Connect to the firewall using the following:

Setting	Value
Speed	Baud 9600
Data Bits	8Bit
Parity	None
Stop Bits	1
Flow Control	No Hardware Flow Control
Com Port	The correct com-port

Step 4. The firewall should then respond with its name or hostname. (If it doesn't try pressing "enter")

Step 5. Reboot the firewall. If there is no power button, disconnect the power adapter and reconnect it after 10 seconds. Plugging in the power too soon after unplugging it can cause corruption in the memory in some units.

Step 6. Wait for the Firewall name and login prompt to appear. The terminal window should display something similar to the following:

```
FortiGate-60C (18:52-06.18.2010)
Ver:04000010
Serial number: FGT60C3G10016011
CPU(00): 525MHz
Total RAM: 512 MB
NAND init... 128 MB
MAC Init... nplite#0
Press any key to display configuration menu...
.....
reading boot image 1163092 bytes.
Initializing firewall...
System is started.
<name of Fortinet Device> login:
```

Step 7. Type in the username: maintainer

Step 8. The password is bcpb + the serial number of the firewall (letters of the serial number are in UPPERCASE format)

Example: bcpbFGT60C3G10016011

Note: On some devices, after the device boots, you have only 14 seconds or less to type in the username and password. It might, therefore, be necessary to have the credentials ready in a text editor, and then copy and paste them into the login screen. There is no indicator of when your time runs out so it is possible that it might take more than one attempt to succeed.

Step 9. Now you should be connected to the firewall. To change the admin password you type the following...

In a unit where vdoms are not enabled:

```
config system admin
edit admin
set password <psswr>
end
```

In a unit where vdoms are enabled:

```
config global
config system admin
edit admin
set password <psswr>
end
```

Warning

Good news and bad news. Some might be worried that there is a backdoor into the system. The maintainer feature/account is enabled by default, but the good news is, if you wish, there is an option to disable this feature. The bad news is that if you disable the feature and lose the password without having someone else that can log in as a superadmin profile user you will be out of options.

If you attempt to use the maintainer account and see the message on the console, "PASSWORD RECOVERY FUNCTIONALITY IS DISABLED", this means that the maintainer account has been disabled.

Disabling the maintainer feature/account

Use the following command in the CLI to change the status of the maintainer account

To disable

```
config system global
    set admin-maintainer disable
end
```

To enable

```
config system global
    set admin-maintainer enable
end
```